Christine A. Jaszkowski - last draft; IDS 2000-0020

From: Joseph P. Krause
To: craig.decaluwe@ftgx.com
Date: 10/6/2000 1:43 PM
Subject: last draft; IDS 2000-0020
CC: Jackson, Thomas; Jaszkowski, Christine A.; rblevy@lga.att.com

Craig,

Here is the most recent draft, which includes both your comments and Bob Levy's comments in RED. In the spirit of Bob's revisions, you'll note that I removed all references to "sabotage" and substituted more oblique language to data overload.

Thanks for your comments. My assistant & I will be in touch soon with the formal papers.

Joe

METHOD FOR TRACKING SOURCE AND DESTINATION INTERNET PROTOCOL DATA

FIELD OF THE INVENTION

This invention relates to data networks. In particular this invention relates to a method and an apparatus for managing data flow in an Internet Protocol (IP) network so as to prevent network disruption caused by excessive data flow through one or more switches.

BACKGROUND OF THE INVENTION

Figure 1 depicts a simplified block diagram of a simplified IP data network 100 of the prior art. The IP network 100 allows IP data to be sent between network users 120 and 122. A network of IP routers 102, 104, 106, and 108 (the purpose, function and operation of which are well known in the art) are interconnected by several data paths 110, 112, 114, 116, and 118 such that data from a particular customer 120 can be routed to/from other internet protocol data network customer 122 using any pathway through the network 100 such as coaxial cable, fiber optic cable, microwave data or other appropriate links between the routers.

As an example of a pathway through the network, data from a customer 120 might be received at a first router 108 and routed over a data path 118 to another router 102 which routes the traffic over the pathway 110 to the other router 104 connected to the destination address, customer 122. Alternate pathways through the network 100 might route data from router 108 through router 102 to router 106 and then to router 104. Yet another pathway might exist from router 108 to 106 to 104.

A problem with an IP data network, such as the simplified depiction in Figure 1, is that one or more individual routers or internet protocol data switches can become overloaded by the transmission of data to a particular destination address or the receipt of too much data from a particular source address. ~~Some individuals consider the generation of spurious data, thereby overloading a router, to be a prank.~~ Curtailing or limiting ~~such~~ data to or through a router ~~traffic~~ might ~~help~~ limit the economic losses caused by data that is lost because a router is overloaded. ~~damage caused by such criminal conduct.~~

It is well known that IP data packets include both source and destination addresses, which are numerical indicators of the computer of the network from which the data originated and to which a packet is to be sent. In an internet protocol data system, misdelivered or discarded data packets that are not received by the destination are retransmitted by the source at the request of the destination when expected data packets, identified by other data transmitted with each packet ~~identified by other identifying data transmitted with each packet~~, do not arrive.

Another problem with prior art internet protocol data switching networks is the inability to manage or control the flow of data from a particular source address or to a destination address in order to avoid overloading one or more routers in a network so as to insure the smooth flow of data packets through the overall network. A method and apparatus by which an internet protocol data network can manage the receipt of data from or to an address location would be an improvement over the prior art. ~~, by at least providing a method and apparatus to control or limit damage caused by sabotage.~~

SUMMARY OF THE INVENTION

In an IP data network, source and destination IP addresses are recorded in memory in a router. The data on source and destination addresses of the data packets passing through the router are read through a user interface, or alternatively by a computer, to tabulate the amount of data from and to individual IP source and destination addresses.

When the data traffic from or to a particular IP address exceeds a predetermined threshold rate, the router can be controlled to discard messages either from a particular IP address or to a particular IP address via a user interface.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a simplified block diagram of a prior art internet protocol data network.

Figure 2 shows a simplified block diagram of an exemplary router device with incoming data lines, outgoing data lines and buffer and memory devices by which source and destination IP addresses are tracked and recorded.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 2 shows a simplified block diagram of an improved internet protocol router 200. Incoming data lines 202, 204, and 206 carry internet protocol data packets, not shown, into the router 200; outgoing data lines 210, 212, 214 carry internet protocol (IP) data packets out of the router 200.

As is well known to those skilled in the art, IP data packets resemble Ethernet data packets in that each includes an address known as a source address that identifies a computer from which the data packet was originated. Each IP data packet also includes a

destination address, which uniquely identifies the destination or end point to which the data packet is to be routed and delivered.

In Figure 2, incoming data packets, i.e., data packets arriving on incoming lines 202, 204, or 206, are received at one or more data buffers 208 within the router 200. The data buffers 208 are typically comprised of random access memory (RAM) or equivalent (perhaps an appropriate fast disk drive) and provide an elastic storage for the data packets in the router device 200 that are eventually transmitted on outbound data lines 210, 212, and 214 to other points in the IP network.

While IP data packets are resident in the buffer 208 of the router 200, the source and destination IP addresses within each data packet are copied into or stored into a memory device 216, which acts to accumulate a record of the data traffic through the router 200 over a finite period of time. By using the accumulated data in the memory device 216, a processor, either within the router 200 or outside the router via a user interface 220, tabulates or counts the occurrence of either or both the source addresses and destination addresses of data packets passing through the router 200.

By counting the occurrences of source addresses and/or destination addresses carried through the router 200 over a predetermined time interval, the length of which is a design choice, it is possible to measure the amount of traffic to and/or from a particular IP address so as to prevent data from a particular router, such as the routers 102, 104, 106 or 108 in Figure 1, from overloading another router in the network.

By way of example, so-called computer hackers, intent on frustrating a computer network, might cause massive amounts of spurious data to be generated to or from one or

more other routers in the network. Large numbers of data transmission from one switch (or source address) to another switch (or destination address) might be attributable to many causes. ~~are frequently caused by deliberate acts of sabotage~~. (In most instances, hackers cause many switches to send data to one switch to drive it into overload.) By tracking the data origins and destinations by source and destination addresses, it is possible to prevent such acts from crippling an entire data network if overruns (sometimes referred to as storms of data or data storms) of data are discarded or suppressed.

In Figure 2, a user interface 220, which provides access to the data stored in memory 216, allows the accumulated tally of source addresses and destination addresses to be manually read. If the count of source and destination addresses per unit time exceeds some predetermined threshold, commands entered by the user interface 220 configure the router 200 to ignore IP data packets from, or to, the problematic address.

In an alternate embodiment, data traffic volume to or from a particular source address is monitored automatically. In the unlikely event that the source switching system were to be overloaded by ~~sabotaged so as to generate~~ an overwhelming amount of data for a destination address, an intervening router can inhibit the over-loaded ~~sabotaged~~ switch from bringing a network down by overloading one or more of the intermediate nodes of the network.

In the preferred embodiment, a running count (or tabulation) of data packets received from a source address or to be sent to a destination address can be entered via the user interface 220 to the router itself 200. Alternate embodiments would certainly

include substituting a computer manager for the user interface 220 such that the computer manager 220 would automatically poll the memory 216 over time to monitor the rate at which packets are flowing through the router. In the event the data from a particular address or to another address exceeded some manually or automatically ~~pre~~determined threshold, both of which could be determined either empirically or heuristically, network ~~sabotage~~ congestion might be avoided by manually or automatically suppressing the reception of additional data packets from a particular source or ~~automatically~~ discarding data packets accordingly. For purposes of claim construction, the manual and automatic determination of a threshold at which packets might be suppressed or discarded are considered to be equivalent. Similarly, the manual and automatic suppression of packets is considered to be equivalent.

The action of discarding a data packet can be accomplished simply by ignoring incoming data packets from a source address. Alternative methods would include overriding previously stored data packets in a buffer with newly received data packets such that the end result is that the total volume of data packets from a source does not exceed some predetermined allowable threshold. One or more messages might be sent from one router to another, instructing the other switch to discard packets from a particular source. A variant of such an embodiment would include sending such an alarm message throughout the network so that all switches connected therein would discard problematic data. As for the inhibition of packet transmission, an overwhelmingly large number of data packets addressed to a destination can be controlled simply by deleting or overriding outbound packets with new or other information.

By monitoring the source address data and the destination address data in an IP protocol network, ~~acts of sabotage~~ data overflow on a network might be avoided. By automating the monitoring and maintenance of data traffic through the network, overall system reliability can be increased.

5

We claim:

1. In an Internet Protocol (IP) data network comprised of a plurality of interconnected IP data switching systems, a method comprised of:
   a. receiving at a first IP data switching system a plurality of IP data packets;
   b. tabulating at said first IP data switching system at least the number of IP data packets received from a particular IP source address during a first time interval, thereby forming a count of IP data packets from a particular source;
   c. storing said count of IP data packets in a memory device for subsequent processing.

2. The method of claim 1 further including the step of:
   d. reading said count of IP data packets from said memory device;
   e. selectively discarding IP data packets received at said first IP data switching system that originated from said particular source.

3. The method of claim 1 wherein said IP data switching system is an IP data router switching system.

4. The method of claim 2 wherein said step of selectively discarding IP data packets includes the step of denying reception of IP data packets from a router

based upon a source address in IP data packets upon the determination that the count of IP data packets from a source address exceeds a threshold value.

5. In an Internet Protocol (IP) data network comprised of a plurality of interconnected IP data switching systems, a method comprised of:

a. sending a plurality of IP data packets from a first IP data switching system to a second IP data switching system;

b. tabulating at said first IP data switching system at least the number of IP data packets sent to a particular IP destination address during a first time interval, thereby forming a count of IP data packets sent to a particular IP destination address;

c. storing said count of IP data packets sent to a particular IP destination address in a memory device for subsequent processing.

6. The method of claim 5 further including the step of:

~~f.~~d. reading said count of IP data packets from said memory device;

~~g.~~e. selectively inhibiting the transmission of IP data packets from said first IP data switching system to said second IP data switching system when the number of IP packets from said first IP data switching system exceeds a predetermined number.

7. The method of claim 5 wherein at least one of said first and second IP data switching systems is an IP data router switching system.

8. The method of claim 5 wherein said step of selectively inhibiting the transmission of IP data packets includes the step of sending a message to a specific router to discard messages either received from or sent to a specific IP address.

ABSTRACT OF THE DISCLOSURE

In an IP network, tabulating the number of data packets received from and/or sent to a particular IP address over time can provide a mechanism by which it is possible to determine or predict overloading of a node or nodes in an IP data network. By selectively deleting data packets received from a suspect source address or inhibiting the transmission of data packets to a suspect destination address, network management and control can be readily accomplished.